Security-Related Stress: A Perspective on Information Security Risk Management

Martin Lundgren
Department of Computer Science
Luleå University of Technology
Luleå, Sweden
Martin.Lundgren@ltu.se

Erik Bergström
School of Informatics
University of Skövde
Skövde, Sweden
Erik.Bergstrom@his.se

***Abstract* — In this study, the enactment of information security risk management by novice practitioners is studied by applying an analytical lens of security-related stress. Two organisations were targeted in the study using a case study approach to obtain data about their practices. The study identifies stressors and stress inhibitors in the ISRM process and the supporting ISRM tools and discusses the implications for practitioners. For example, a mismatch between security standards and how they are interpreted in practice has been identified. This mismatch was further found to be strengthened by the design of the used ISRM tools. Those design shortcomings hamper agility since they may enforce a specific workflow or may restrict documentation. The study concludes that security-related stress can provide additional insight into security-novice practitioners' ISRM challenges.**

Keywords — Information security, information security risk management, novices, stress, tools, compliance, management

I. Introduction

Information Security Risk Management (ISRM) is relevant for organisations looking at expanding their operational capacity through digitalisation [1]. Digitalisation has impacted the way real-time information can be exchanged globally, and many organisations have embraced the innovation of new services as part of their competitive advantage and growth [2], [3]. Digitalisation thus holds many opportunities, but with this development, new types of risks have emerged. The effective consumption and reliable production of information that comes with digital services has become an increased target of cybercriminal activities [1]. Hence, to exploit these opportunities, it is important first to assess the risks they hold.

ISRM is the continuous process of identifying and countering security risks to the availability, confidentiality and integrity of information [4], [5]. The literature often depicts ISRM as activities performed in a rational, predominantly instrumental, fashion [6]. Considering information being among an organisation's most critical business resources [7], the role and importance of ISRM as an integral part of an organisation's digital development and growth should be noted. This need for security has also been recognised by practitioners, researchers, and lawmakers, as well as end-users trusting the services [8], [9], [10]. As a result, ISRM has received much research attention. This has, in turn, resulted in numerous standards for how to conduct ISRM [11], alongside the development of various tools to aid its enactment [12]. Such tools could be, for example, worksheets, document templates, or software designed to assist in the ISRM process and to elaborate on its activities [12], [13].

While there is literature on how practitioners should conduct ISRM, there is little on how they actually perform ISRM [14]. Additionally, there is not much research on ISRM from a security-novice perspective [15]. Previous studies have, however, highlighted, for some time, concerns among organisations with limited security awareness or experience when deciding about or developing their digital services [15], [16]. Osborn and Simpson [15], for example, found that novice practitioners were uncertain about developing or outsourcing digital services because they felt they lacked the understanding of the consequences and limitations of the developed services or agreed contracts. Although security has become an important part for many organisations, a lack of security skills, perception or awareness can make ISRM processes complex and difficult to understand and follow [15], something that could cause "Security-Related Stress" (SRS) [17].

SRS was originally used to explore end-users' security violations caused by burdensome, complex, and ambiguous information security requirements [17]. In their study, D'Arcy, Herath and Shoss [17] argue that end-users' lack of security experience and knowledge, and the security requirements demanded of them, could result in SRS and influence their security decisions. Considering that many ISRM processes have been shown to require a great amount of expertise to apply [13], [14], it is unclear if and how ISRM is similarly affected by security-novice practitioners' SRS. In this study, therefore, this research stream is furthered by exploring security-novice practitioners' enactment of ISRM, using SRS as an analytical lens. A case study was performed in which two security-novice organisations were observed during the starting of their ISRM activities. We further discuss and propose potential benefits and disadvantages of using tools to help perform various ISRM activities.

The study is outlined as follows. Section II introduces the background on ISRM processes and discusses tools designed to aid its practical enactment and SRS. Section III presents the research approach, followed by Section IV, which presents the empirical results. This is followed by Section V, which discusses the results, and finally, Section VI highlights the study's conclusions and implications.

II. Background

A. Information Security Risk Management Processes

As outlined above, ISRM is the overall process to analyse and address risks to an organisation's confidentiality, integrity, and availability of information. ISRM processes have been described in numerous standards and scientific work alike [5], [18], [19], each developed to meet its particular need with different objectives and activities [20]. However, this has also led to some confusion regarding the meaning of ISRM [21], and many, subtly different, definitions of its activities [22]. For example, a common ISRM standard such as ISO/IEC 27005 [23] includes context

establishment, risk assessment, risk treatment, and risk monitoring and review in its ISRM process, with various additional sub-activities. Another example is NIST SP 800-30 [24] in which the process consists of risk framing, risk assessing, risk response, and risk monitoring. While authors such as Spears and Barki [25] describe the ISRM process as consisting of identifying and prioritising risk and implementing and monitoring controls, others such as Straub and Welke [26] describe the process as consisting of activities to recognise security problems, perform risk analysis, generate security control alternatives, decide on security controls, and implement the selected security controls.

Although various ISRM processes differ in scope, depth and particular steps, they usually share some similar activities like the identification and valuation of assets, analysis of risks, and the mitigation of risks to reach an acceptable level [4], [14], [27], [28]. Therefore, ISRM in this study is described as giving a general view and structure, not adhering to any particular standard or process and being comprised of asset valuation, risk analysis and selection of security controls. These have also been recognised as the basic ISRM activities [29].

However, for many ISRM processes, it is common that their activities are often described as if performed in a predominantly instrumental fashion [6]. The risks to information assets are thus often portrayed as something that can be controlled if managed rationally [30], [31]. In this approach, the output of the asset valuation typically serves as the input for the risk analysis. For each asset, a risk analysis is performed to identify and evaluate risks based on an estimation of vulnerabilities in systems and environments, the likelihood of a particular threat exploiting those vulnerabilities, and the criticality of the assets [21]. The resulting estimation is what enables a rational decision regarding what risks to mitigate, and what risks to accept. In addition, it is also common to include some form of feedback operation that carries historical risk mitigation data, such as incidents, to continuously improve the level of protection and threat relevance [32], [33].

B. *Information Security Risk Management Tools*

While the implied order of activities found in standards can provide a valuable frame of reference regarding ISRM implementation, it could stifle organisational flexibility and fit if interpreted as a blueprint of reality [6]. This is further amplified by ISRM tools designed to serve as guidance for activities, which could give the perception that the activities are static and not dynamic. Over the years, several tools have been developed, many of which are designed to conform with particular standards and their respective activities and which are outlined in a series of steps [12].

However, tools can only help so much. Ultimately, tools depend on the input data captured and provided by the practitioner, alongside their understanding of definitions and requirements, which have often proven to be too technical or ambiguous for the security-novice [13]. For example, both standards and tools often fall short in answering fundamental questions like how to perform this data collection, what counts as critical and non-critical assets, or how the likelihood of a threat can be estimated [13], [20]. Furthermore, tools sometimes come with certain design restrictions or limitations, which can burden future ISRM developments. For example, in their meta-study on ISRM tools, Gritzalis, Iseppi, Mylonas and Stavrou [12] found examples of restrictive limits of characters allowed to be entered and saved in the tool, which could lead to useful data being undocumented and lost. Yet, human motivational elements are mostly neglected [34], and many tools thus require good, or even expert, experience and knowledge to be used [12]. However, considering that it is often the on-site personnel and non-experts who conduct ISRM, additional work is needed to develop tools and activities that can make ISRM more efficient [13]. Otherwise, ISRM activities and tools designed to ease its conduction could result in the opposite and instead end up burdening the entire process and risk causing SRS.

C. *Security-Related Stress*

Stress is a very broad research topic [35]. Stress-related research within the field of information systems has traditionally been directed at investigating stress experienced by ICT professionals and not on how technology can be a source of stress (i.e., technostress) [35], [36]. Technostress can describe the end-user stress caused by a workplace full of accelerating technology demands [35], [37]. Building on the concept of technostress, D'Arcy, Herath and Shoss [17] use the term Security-Related Stress (SRS) to describe the stressful demands specifically imposed by security requirements. D'Arcy, Herath and Shoss [17] describe SRS as "caused by internal or external security-related demands appraised as taxing one's cognitive resources or abilities" [17 pp. 288]. Based on an information systems security context, D'Arcy, Herath and Shoss [17] describe three relevant dimensions of stress as; overload, complexity, and uncertainty. Based on the work of Ragu-Nathan, Tarafdar, Ragu-Nathan and Tu [36] and D'Arcy, Herath and Shoss [17], these dimensions are conceptualised from an ISRM perspective, from which the respective dimensions are described below.

Overload can be described as stressors stemming from situations in which security-related requirements increase the workload for ISRM practitioners, resulting in added time pressures for them to complete their job duties [17]. Security requirements are often seen as laborious and an unnecessary overhead that hinders productivity [38], [39]. Many practitioners in the ISRM process do not work exclusively with information security, but rather have other main duties, adding extra stress to their situation. Participation in valuations or risk analyses, are examples of extra work that causes stress.

Complexity can be described as stressors stemming from situations in which security requirements are viewed as complex, forcing ISRM practitioners to spend time and effort in learning and understanding security [17]. Examples include checklists, tools, and documentation containing technical or information security jargon [40] that causes ISRM practitioners to halt and become forced to read-up to be able to make informed decisions. For example, the ISO/IEC 27005 [23] standard has been found to be both challenging to read and hard to grasp for novices [13]. This, in turn, causes ISRM practitioners to spend time and energy on extra tasks, thus causing stress.

Uncertainty can be described as stressors stemming from situations in which security requirements in the organisation continually change and are updated [17]. The new

requirements can be internally driven or a result of government or industry regulations [17]. There are numerous examples, in which new requirements affect security, e.g., with the introduction of the Directive on security of network and information systems (NIS) [41] and the General Data Protection Regulation [42] in the European Union. Uncertainty can also come from mandatory periodical security training, changes in security tools, and constantly changing risks that the organisation is facing. The dynamics of all these changes cause ISRM practitioners to constantly adjust to new requirements, causing uncertainty, and in the end, stress.

It is important to acknowledge that for each SRS dimension, there can be "stressors" as well as "stress inhibitors". Stressors are the creators of stress, i.e., factors that create stress from the ISRM perspective. Stress inhibitors, on the other hand, are means that reduce the level of stress [36], i.e., organisational mechanisms that lower stress from the ISRM perspective.

III. Research Approach

To be able to investigate the starting of an ISRM process, and the enactment of its activities, a case study aimed at interpretation, as described by Braa and Vidgen [43], was set up. The case study was inspired by the protocol described by Yin [44]. More specifically, an analytical SRS lens consisting of the three dimensions with each corresponding stress inhibitor was first developed. Since the novice ISRM practitioner's enactment was in focus, a University level commissioned ISRM education was contacted. Through this education, two public sector organisations, here labelled as Alpha and Beta, were interested in participating in observations, interviews, and giving access to their internal ISRM documentation such as policies and procedures.

Alpha is owned by 39 Swedish municipalities and one regional council, and Beta is a medium-sized Swedish municipality. Alpha provides services critical for citizens, and Beta, as a municipality, provides many functions and maintains infrastructure critical to society. Both Alpha and Beta have in the last years been affected by new requirements coming from the GDPR and the NIS directive. Striving to achieve information security, both Alpha and Beta have chosen to implement an ISRM process but are still early in their respective processes.

As a first step, both Alpha's and Beta's internal ISRM documentation describing their approaches to valuation and risk analysis were collected and analysed to get insights into their respective ISRM processes. The analysis of the documentation together with the dimensions of SRS formed the basis of the interview guide used for the open-ended questions encouraging the respondent to provide an extensive answer [45].

The observations followed and were conducted for both Alpha and Beta in a series of workshops. Each workshop focused on a particular ISRM activity such as valuation or risk analysis and was led by a manager who was assigned as the workshop leader. These workshop leaders were themselves novices and participated in the ISRM education described above. The authors recorded everything with video and acted as complete observers, meaning that they took no part in the workshops [45].

Directly following the last observations, group interviews with Alpha and Beta were held, using the interview guide. The questions targeted clarifying questions, e.g., about their documentation practices, and more reflective questions about the enactment, such as "what are your views on the valuation conducted today?" To get more insights into the organisations' work practices, joint group interviews, including respondents from both Alpha and Beta, were held a few weeks after the observations. In this joint session, the managers who had participated previously in the observations and group interviews were invited. The nature of this joint group interview was to further elaborate on some aspects such as their views on the ISRM process, its activities, how tool usage affected them and compliance. An overview of the data collection can be seen in Table I.

TABLE I. An overview of the data collection.

Type of Data Collection	Respondents and Quantity	Transcribed/ Collected
4 observations	Alpha: 5 workshop participants Beta: 6 workshop participants 5 hours in total	7 pages
2 group interviews	Alpha: 5 respondents Beta: 6 respondents 1 hour and 15 minutes in total	2 pages
1 joint group interview	4 respondents from Alpha and Beta 1 hour	8 pages
ISRM documentation	10 documents in total	76 pages

The observations and interviews were individual and partially transcribed by the authors, with a focus on the SRS dimensions. Other data were omitted from the transcripts. For the data analysis, the SRS dimensions were used as predefined codes, i.e., overload, complexity, and uncertainty, together with each corresponding stress inhibitor. The data analysis was performed in three steps, based on qualitative content analysis [46]. First, each author identified chunks of text in the transcripts corresponding to any of the codes. These chunks were then joined, sorted, and grouped based on the codes. Next, the authors examined the content of each code and extracted key concepts representing the codes jointly. Finally, each key concept was synthesised into a coherent text with associated descriptions.

IV. Empirical Results

The SRS dimensions, i.e., overload, complexity, and uncertainty are each presented together with their corresponding stress inhibitors in separate sections. An overview of the empirical results is outlined in Table II.

TABLE II. An overview of the Empirical Results.

SRS Dimension	Stressors and Stress Inhibitors
Overload stressors	– Tools promote sequential rather than agile workflow – Lacking time and resources to work with ISRM
Overload inhibitors	– Tools translating information value to security controls – Direct relation between information value and security controls was experienced as time saving
Complexity stressors	– Mismatch in language used in ISRM documentation, the organisation and the tool – Too comprehensive ISRM documentation
Complexity inhibitors	– Walkthrough of the entire ISRM process to cover aims and objectives

	– Workshop leader preparing an embryo of possible information types to aid the start of the valuation
Uncertainty stressors	– External requirements (such as laws and regulations) – Mismatch between assumed work practices, ISRM documentation and use of tools – Lack of tool functionality, e.g., for documentation
Uncertainty inhibitor	– Workarounds in tool usage to fit work practices

A. Overload

The overload dimension was seen in both organisations in various forms, both as a part of the tools they used and the user's participation. Both organisations used existing tools and templates in varying degrees to help them perform and document the ISRM process. These were based on Microsoft Excel and Word and differed between the two organisations. In addition, both organisations used the same online tool, called "Klassa" [47], to help with the valuation. Klassa is a free-to-use Swedish public sector initiative aimed at supporting the ISRM process by helping to identify categories of potentially missing security controls, based on the information value and legal nature. Klassa is developed to support the valuation of systems containing assets, rather than the individual assets themselves, in an approach similar to the one described by Fibikova and Müller [48]. Based on the valuation of the system, the existing security controls, laws and regulations affecting the information in the system, and the system itself, missing security controls are identified and serve as the output of the tool. Alpha finds that using a tool like Klassa alleviates for them the difficulty of translating information value to security controls, in effect acting as a stress inhibitor.

While both organisations used Klassa, the tool was perceived and used differently in two ways. First, the resulting list of categories of security controls was seen differently. In Alpha's case, the list represented a list of suggestions, and security controls to be addressed where needed. Beta, on the other hand, sees the result as a list of requirements to be implemented as is and not as categories of controls. Second, Alpha used Klassa as a support, and the result as they saw relevant: "based on the items in this list, we must see 'are these relevant, or not?', but it is a great way to get started."

Beta centred their work process around Klassa, which required several additional steps to import and export results between Excel and Klassa, in effect having Klassa shape their process rather than supporting it. Beta's Excel tool was separated into different spreadsheets, one for valuation, one for the resulting list imported from Klassa, the third one for risk analysis, and a final one to put together a report. Each of these sheets are interlinked, serving as input and output for each other and thus promoting a sequential, rather than agile, workflow. Alpha's tool, on the other hand, did not dictate a particular workflow, allowing more agility. However, the workflow often implied in standards inhibited them from adapting to situations more agilely. For example, one participant from Alpha recognised that they should not discuss risks during the valuation, i.e., by looking at the consequence rather than the likelihood. However, in the observation, it was clear that the workshop participants drifted into the risk analysis in order to land at a more correct valuation. At times, they would recognise that they were talking risks during the valuation, and discontinued their discussion, in effect discarding any identified risks since "they [the risks] will be shown later in the risk analysis." Later, during the group interview, one participant explained that it would benefit them to talk risks during valuation, since "it comes as a natural step to think about risks during the valuation."

One interesting aspect of using Klassa is that it provides a direct relation between information value and security controls and does not necessarily decrease the workload. In Alpha's case, this relation informs their valuation, meaning that Alpha adjusts their valuation based on the consequential amount of security controls in which it would result. At one point, Alpha exclaimed that "In the worst case, we might end up with a three [highest valuation level]", referring to the fact that a higher valuation will result in a more detailed list of security controls to consider than initially expected. In a similar attempt to decrease the workload, Beta encourages a rapid rather than precise approach, "It is approximately 100 questions, so it is important to have tempo, tempo, tempo,... use your gut feeling." In the joint group interviews, the long lists with questions were discussed, and several suggestions on how to decrease the burden from a tool perspective were suggested by the respondents. For example, if the infrastructure is already valued and has received security controls accordingly, many questions in Klassa could be removed. Hence a more agile approach in the tool could decrease the time spent on the valuation.

In both Alpha's and Beta's cases, adding time and pressure to complete job duties, because they do not work exclusively with security, adds stress to their daily work. For example, during the group interview when questioned about their opinions on finding security controls, one participant from Beta complained that "well, this is not exactly the only thing we do" in reference to participating in the ISRM process. Similarly, in Alpha's case, one participant explained that "we cannot have a situation where our organisation gets affected by us sitting and doing risk analysis' all the time [...] perhaps it's a good thing during these major changes [the procurement of a new system]" in reference to her participation in the ISRM process. In the joint group interview, lacking resources and time-saving measures were discussed, and one example that was emphasised was the direct relationship between information value and the security controls, or as one of the respondents put it "by connecting information value to security controls... maximises [time utilisation]".

B. Complexity

To decrease complexity, both Alpha and Beta started their respective workshops with a walkthrough covering the aims and objectives of their entire ISRM process. This assisted in bringing the workshop participants up to speed on what to do and how to get started. Similarly, during the joint group interview, the respondents also reflected on this type of introduction as being a good way to introduce workshop participants and raise their awareness about the ISRM activities about to be conducted in the workshop.

However, during the observation, several indications were given by the workshop participants at Alpha and Beta about the difficulties in getting their respective ISRM cases started. For example, Alpha had a long discussion about their systems and information flow, trying to find a starting point for their valuation. This discussion was expected by the workshop leader, who had prepared a list of possible

information types (e.g., customer data and log data) to be used as a starting point, despite lacking insights into the specifics of the systems. While this level of detail started a discussion on trying to identify correct information types, they, in the end, reached a valuation decision based on the system itself, rather than on all the discussed information types. In the interviews, the workshop leader was asked why this happened, and he replied: "well, I must admit that I had them [the information types] in the back of my head during the process, and maybe we should have been more systematic valuing all the information types." The motivation behind this was to get the discussions going. However, this also led to much information not being documented, for example, the motivation behind valuation decisions or various identified information types within the valued systems. This was expressed as a downside of Alpha's tool, "you cannot really write any contextual information describing what the reasoning behind this valuation was", and as a result, had led them to create their separate document to carry such motivations. Although Alpha recognised that this added some additional time and complexity, they justified this by "in the long run, it will be much easier to re-valuation in a year or two, to go back and see 'how did we think back then?'"

Beta, on the other hand, had difficulties not only in getting started but also in getting organisational acceptance of their ISRM approach. Beta's initial approach was in their words "more complete" and included a more comprehensive ISRM process. However, this approach "was actively rejected by more or less everybody" due to its comprehensiveness since it "became far too extensive and complicated". As a result, Beta developed two additional, simplified, versions of the valuation to speed-up the ISRM process. However, this did little to help in practice, since choosing one of these simplified approaches was shown to be difficult, considering the selection itself depended on a firm understanding of the value of information. The respondents suggested that the main motivation behind the three approaches was to stay compliant, "doing something", rather than to increase security by having a sufficient ISRM process.

One aspect of the tool use that caused complexity was the language barrier. The language in the tool Klassa, as the tool used by both Alpha and Beta, did not match the language used in their respective organisations, and during the observations, discussions halted several times so the workshop participants could discuss definitions of terms. Furthermore, at Beta, there were ambiguities in how to interpret the wording in Klassa, for example, discussions around what is included in "measures to prevent and minimise operational disruptions are implemented", and "technical and organisational measures are taken to manage identified risks."

Finally, discussions in the joint group interviews touched on the topic of standardising security controls for certain information types nationally or internationally. Furthermore, it was discussed that certain types of systems have great similarities regarding information types, and hence tools could support information identification by giving examples of typical information types to decrease complexity.

C. *Uncertainty*

In both Alpha's and Beta's cases, much of their ISRM work was externally motivated by the introduction of the NIS directive and GDPR, mandating a more systematic approach towards information security. During the observations, several indications were shown that suggested both organisations were in the early phases of establishing their processes. For example, the previously described direct relation between valuation and security controls, provided through the tool Klassa, was used as a stress inhibitor, since security controls for a particular information value are given. This was further discussed during the joint group interview, that it could be of help to have standardised security controls for a given type of information, covering both national and international requirements. However, this could also cause uncertainty, since the given set of security controls are externally defined, and in its nature, independent of context. For example, adapting to these, as is, could cause ambiguity in required security requirements. In Beta's case, one such example was the resulting security control "Measures to prevent and minimise operational disturbances have been implemented", which was adopted into their risk analysis as is, and its security control noted as "Do this".

Other indications were found in both organisations that suggested the early development of their respective ISRM processes. Their approach to the ISRM activities indicated a mismatch between assumed work practices, their policy and use of tools. For example, Alpha's template for documenting the valuation included procedures for how they should conduct valuation, but these procedures did not correlate with their actual enactment. In practice, the tool did not support the flow of their work and discussions, and instead, interrupted it by having the workshop participants go back and forth in the tool to find the right sections. This focused much of their attention on the tool itself, rather than continuing and documenting their discussion. One example from Beta of how the tool lacked in supporting their work process came when filling in a long checklist in Klassa. The workshop participants were advised to either ask colleagues for help or in Klassa to fill in 'does not fulfil the requirement at all' if they are unsure about a question. Since all questions marked 'does not fulfil the requirement at all' will be tagged, it will work as a reminder in practice. The tool is not designed with any feature supporting saving questions to be discussed at a later stage, but it is needed, and hence a workaround is created. In the interviews, one of the respondents even reflected over this practice by stating that "this feature 'does not fulfil the requirement at all' is very good, so you know where the gaps are."

When it comes to the documentation of the ISRM work, both organisations acknowledged the lack of support from both the tool and their internal information management systems. The information saved in Klassa was deemed insufficient, as the reasoning behind decisions, normally expressed as contextual information, was not possible, and hence additional documentation was necessary. Both Alpha and Beta sent their ISRM documentation to their respective central organisational archiving functions. Alpha expressed that they "do not have a great information management system" and that by using their central archiving function, "at least it is saved somewhere."

V. Discussion

While there is much research on what should be done with regard to ISRM, much of it has been shown to require a great amount of expertise to apply [13], [14]. In this study, SRS [17] was used as an analytical lens to investigate the enactment of ISRM by novice practitioners. It is reasonable to argue that SRS is a valid analytical lens to study novice practitioners, as a lack of security experience could cause overload, complexity and uncertainty. These dimensions of SRS gave additional insights into what challenges ISRM processes pose, which may not be evident for practitioners with more experience and could thus help in developing standards and tools to be more available for organisations perhaps not solely devoted to security issues. For example, our findings point to the potential benefits and disadvantages of using tools to help perform various ISRM activities. Perhaps the most obvious is the experienced inflexibility in workflow and the inherent design of tools to support compliance, the difficulties in getting started, and limitations in what and how to document.

Throughout the observations, it was clear that the tools determined the ISRM process. Beta went so far as to design their work process around the online tool that they used. Although Alpha used the same online tool, they allowed for a more agile approach, but still seemed reluctant to do so, as if it would be wrong of them to perform ISRM activities in parallel, for example. An inadvertent gravitation, perhaps, towards including and conducting activities to ensure compliance with a particular standard. However, while it makes sense to perform ISRM activities chronologically, interpreting it as a blueprint of reality could burden the actual process enacted in practice, since it might not fit the current organisational context. Standards such as the ISO/IEC 27001 [18] stress that the ISRM process should be adapted to the organisation. However, this adaption requires a certain level of experience, since standards are designed to be universal in scope and thus leave much to be interpreted by the practitioner. The resulting ambiguity is a good example of an SRS complexity trigger. Take Alpha for example; in their interpretation, risks ought not to be discussed during valuation, which resulted in them discouraging their discussion and leaving it undocumented, even though they exclaimed it could have helped them.

However, the tools observed did not seem to help aid the workshop participants contextualising their ISRM process to fit the organisational needs. Instead, tools were seen as designed to strictly follow a pre-determined progression of ISRM activities. In effect, following the tools were interpreted as synonymous with being secure. This is consistent with Kwon and Johnson [49], and Webb, Maynard, Ahmad and Shanks [50], who found that there is a growing misconception that compliance with formal processes is equivalent to good security. This was further seen in the case of Beta, which was motivated in their choice of methods as a means to stay compliant, rather than developing and adapting the ISRM process to tailor it to their organisational fit. In the joint group interview, compliance was discussed, and it was accepted that sometimes "good enough" [51] is sufficient to cope with the SRS burden. That is, to know what level of abstraction is manageable in their context to reach compliance, rather than to get stuck in long discussions overdoing the level of details.

The limitations in knowing, deciding, and understanding what to document and how to document it was evident from the two cases. The tool Klassa lacked possibilities to add contextual information, e.g., the underlying motivations for the valuation and information on stakeholders handling the information, which is also an important input to the risk analysis. The transition from valuation to risk has proven troublesome [52], [53], and the contextual information could potentially be more valuable than the actual valuation result at a future re-valuation [6]. Lacking these possibilities, combined with a reluctance to save information in the cloud, meant that both organisations documented their ISRM results in various documents related to the valuation and risk analysis that in the end were sent to a central archive. These approaches inhibit the overall ISRM process as the results are fragmented, and an overview of all valued systems, identified risks and security controls is missing, which creates more work and hence could result in more SRS.

VI. Conclusion

The purpose of this study was to explore security-novice practitioners' starting with ISRM and their enactment of its activities, using SRS as an analytical lens. It was found that studying novice ISRM practitioners from an SRS perspective highlighted the implications for research and standard developers alike. One such example was the mismatches in how standards are conceived and how they are interpreted in practice. This mismatch was further amplified by the tools supporting the ISRM process, both when performing activities such as valuation, risk analysis and the selection of security controls but also when working with the overall ISRM process. For example, it was shown that tools could force the use of a particular process that was not aligned with the organisation, in effect stifling agility among the observed ISRM practitioners. The study further showed that design restrictions and limitations of tools could cause practical difficulties, such as the documentation of the ISRM process. In the observations, many of the difficulties related to documentation resulted not only in ad-hoc and inefficient practices but also in future developments such as the reuse of previous valuations of the same or similar information types, which otherwise could have been encouraged from a tool perspective.

This study also extends SRS research and shows that D'Arcy, Herath and Shoss's [17] SRS dimensions can be applied to the ISRM field. Understanding how SRS affects ISRM practitioners and how they are coping with SRS through various SRS inhibitors is important and can help advance tool design, processes, and procedures related to ISRM. Several examples of SRS inhibitors were observed, e.g., the direct relation between valuation and security controls that provided a set of controls depending on the valuation is an example of such inhibitors. There are potentially several other SRS inhibitors related to the difficulties of identifying information types, and in deciding what to value, which better fitting tools could support.

This study indicates, by its in-depth approach in two organisations, some future research issues that can be addressed. One such example is the sample size, and similar studies in a larger context could further build on the results presented here. Similarly, additional comparative studies of ISRM processes and tools are advised for further research and development. Finally, additional work is needed to better

understand the challenges faced by novice practitioners and to help develop standards and tools.

ACKNOWLEDGEMENT

Financing for the CYNIC project (20201650) from the EU program INTERREG North 2014-2020 – which supports cross-border collaboration to strengthen competitiveness and attractiveness in and between northern Sweden, northern Finland, northern Norway and Sápmi, and Region Norrbotten as well as Lapin Liitto – is gratefully acknowledged.

REFERENCES

[1] N.-B. Schirrmacher, J. Ondrus, and F. T. C. Tan, "Towards a Response to Ransomware: Examining Digital Capabilities of the WannaCry Attack", in Proceedings from PACIS, 2018.

[2] M. Barrett, E. Davidson, J. Prabhu, and S. L. Vargo, "Service innovation in the digital age: key contributions and future directions", MIS Q., vol. 39, no. 1, pp. 135-154, 2015.

[3] R. Gulati and T. Soni, "Digitization: A strategic key to business", Journal of Advances in Business management, vol. 1, no. 2, pp. 60-67, 2015.

[4] V. Visintine, "An introduction to information risk assessment", SANS institute, vol. 8, 2003.

[5] M. E. Whitman and H. J. Mattord, Principles of Information Security, Fifth ed. Cengage Learning, 2014.

[6] M. Lundgren and E. Bergström, "Dynamic Interplay in the Information Security Risk Management Process", International Journal of Risk Assessment and Management (IJRAM), 2019, in press.

[7] J. S. Broderick, "Information Security Risk Management — When Should It be Managed?", Information Security Technical Report, vol. 6, no. 3, pp. 12-18, 2001.

[8] S. Goel and V. Chen, "Can business process reengineering lead to security vulnerabilities: Analyzing the reengineered process", International Journal of Production Economics, vol. 115, no. 1, pp. 104-112, 2008.

[9] D. J. Kim, M.-S. Yim, V. Sugumaran, and H. R. Rao, "Web assurance seal services, trust and consumers' concerns: an investigation of e-commerce transaction intentions across two nations", European Journal of Information Systems, vol. 25, no. 3, pp. 252-273, 2016.

[10] D. Lekkas, S. K. Katsikas, D. D. Spinellis, P. Gladychev, and A. Patel, "User requirements of trusted third parties in Europe", Proceedings, User identification and Privacy Protection Joint IFIP WG, vol. 8, pp. 229-242, 1999.

[11] C. Gikas, "A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards", Information Security Journal: A Global Perspective, vol. 19, no. 3, pp. 132-141, 2010.

[12] D. Gritzalis, G. Iseppi, A. Mylonas, and V. Stavrou, "Exiting the Risk Assessment Maze: A Meta-Survey", ACM Comput. Surv., vol. 51, no. 1, pp. 1-30, 2018.

[13] G. Wangen, "Information Security Risk Assessment: A Method Comparison", Computer, vol. 50, no. 4, pp. 52-61, 2017.

[14] P. Shedden, W. Smith, and A. Ahmad, "Information security risk assessment: towards a business practice perspective", presented at the Australian Information Security Management Conference 2010, 2010.

[15] E. Osborn and A. Simpson, "Risk and the Small-Scale Cyber Security Decision Making Dialogue—a UK Case Study", The Computer Journal, vol. 61, no. 4, pp. 472-495, 2018.

[16] L. Labuschagne and J. H. P. Eloff, "Electronic commerce: the information ‐ security challenge", Information Management & Computer Security, vol. 8, no. 3, pp. 154-157, 2000.

[17] J. D'Arcy, T. Herath, and M. K. Shoss, "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective", Journal of Management Information Systems, vol. 31, no. 2, pp. 285-318, 2014.

[18] Information technology – Security techniques – Information security management systems – Requirements, 2013.

[19] M. Siponen and R. Willison, "Information security management standards: Problems and solutions", Information & Management, vol. 46, no. 5, pp. 267-270, 2009.

[20] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, "Taxonomy of information security risk assessment (ISRA)", Computers & Security, vol. 57, pp. 14-30, 2016.

[21] M. Gerber and R. von Solms, "Management of risk in the information age", Computers & Security, vol. 24, no. 1, pp. 16-30, 2005.

[22] L. Pan and A. Tomlinson, "A systematic review of information security risk assessment", International Journal of Safety and Security Engineering, vol. 6, no. 2, pp. 270-281, 2016.

[23] ISO/IEC 27005, "Information technology – Security techniques – Information security risk management", ISO/IEC 2013.

[24] NIST SP 800-30, "Guide for Conducting Risk Assessments", National Institute of Standards and Technology, Gaithersburg, MD 2012.

[25] J. L. Spears and H. Barki, "User participation in information systems security risk management", MIS Quarterly, vol. 34, no. 3, pp. 503-522, 2010.

[26] D. W. Straub and R. J. Welke, "Coping with Systems Risk: Security Planning Models for Management Decision Making", MIS Quarterly, vol. 22, no. 4, pp. 441-469, 1998.

[27] M. E. Whitman and H. J. Mattord, Management of information security, Fourth Edition ed. Stamford, CT: Cengage Learning, 2013.

[28] R. Baskerville, P. Spagnoletti, and J. Kim, "Incident-centered information security: Managing a strategic balance between prevention and response", Information & Management, vol. 51, no. 1, pp. 138-151, 2014.

[29] M. S. Saleh and A. Alfantookh, "A new comprehensive framework for enterprise information security risk management", Applied Computing and Informatics, vol. 9, no. 2, pp. 107-118, 2011.

[30] L. Coles-Kemp, "Information security management: An entangled research challenge", Information Security Technical Report, vol. 14, no. 4, pp. 181-185, 2009.

[31] G. Dhillon and J. Backhouse, "Current directions in IS security research: towards socio-organizational perspectives", Information Systems Journal, vol. 11, no. 2, pp. 127-153, 2001.

[32] A. Ahmad, J. Hadgkiss, and A. B. Ruighaver, "Incident response teams – Challenges in supporting the organisational security function", Computers & Security, vol. 31, no. 5, pp. 643-652, 2012.

[33] J. Webb, A. Ahmad, S. B. Maynard, and G. Shanks, "A situation awareness model for information security risk management", Computers & Security, vol. 44, pp. 1-15, 2014/07/01/ 2014.

[34] G. Wangen, C. Hallstensen, and E. Snekkenes, "A framework for estimating information security risk assessment method completeness", International Journal of Information Security, journal article vol. 17, no. 6, pp. 681-699, 2018.

[35] R. Ayyagari, V. Grover, and R. Purvis, "Technostress: technological antecedents and implications", MIS Q., vol. 35, no. 4, pp. 831-858, 2011.

[36] T. S. Ragu-Nathan, M. Tarafdar, B. S. Ragu-Nathan, and Q. Tu, "The Consequences of Technostress for End Users in Organizations: Conceptual Development and Empirical Validation", Information Systems Research, vol. 19, no. 4, pp. 417-433, 2008.

[37] M. Tarafdar, Q. Tu, and T. S. Ragu-Nathan, "Impact of Technostress on End-User Satisfaction and Performance", Journal of Management Information Systems, vol. 27, no. 3, pp. 303-334, 2010.

[38] S. Goel and I. N. Chengalur-Smith, "Metrics for characterizing the form of security policies", The Journal of Strategic Information Systems, vol. 19, no. 4, pp. 281-295, 2010.

[39] C. Posey, R. J. Bennett, and T. L. Roberts, "Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes", Computers & Security, vol. 30, no. 6, pp. 486-497, 2011.

[40] P. Puhakainen and M. Siponen, "Improving employees' compliance through information systems security training: an action research study", MIS Q., vol. 34, no. 4, pp. 757-778, 2010.

[41] The Directive on security of network and information systems (NIS), "Directive (EU) 2016/1148", Official Journal of the European Union, vol. 194, pp. 1-30, 2016.

[42] General Data Protection Regulation, "Regulation (EU) 2016/679", Official Journal of the European Union, vol. 119, pp. 1-88, 2016.

[43] K. Braa and R. Vidgen, "Interpretation, intervention, and reduction in the organizational laboratory: a framework for in-context information system research", Accounting, Management and Information Technologies, vol. 9, no. 1, pp. 25-47, 1999.

[44] R. Yin, Case Study Research : Design and Methods, Third edition ed. Sage Publications, 2003.

[45] B. J. Oates, Researching Information Systems and Computing. London: Sage, 2006.

[46] J. Y. Cho and E.-H. Lee, "Reducing confusion about grounded theory and qualitative content analysis: Similarities and differences", The Qualitative Report, vol. 19, no. 32, p. 1, 2014.

[47] Sveriges Kommuner och Landsting. (2019). Informationsklassning och handlingsplan [Information classification and action plan]. Available: https://klassa-info.skl.se/

[48] L. Fibikova and R. Müller, "A Simplified Approach for Classifying Applications", in ISSE 2010 Securing Electronic Business Processes, N. R. Pohlmann, Helmut; Schneider, Wolfgang, Ed.: Vieweg+Teubner, 2011, pp. 39-49.

[49] J. Kwon and M. E. Johnson, "Health-Care Security Strategies for Data Protection and Regulatory Compliance", Journal of Management Information Systems, vol. 30, no. 2, pp. 41-66, 2013.

[50] J. Webb, S. B. Maynard, A. Ahmad, and G. Shanks, "Foundations for an Intelligence-driven Information Security Risk-management System", JITTA: Journal of Information Technology Theory and Application, vol. 17, no. 3, p. 25, 2016.

[51] E. Bergström, M. Lundgren, and Å. Ericson, "Revisiting Information Security Risk Management Challenges: A Practice Perspective", Information and Computer Security, 2019, in press.

[52] M. Sajko, K. Rabuzin, and M. Bača, "How to calculate information value for effective security risk assessment", Journal of Information and Organizational Sciences, vol. 30, no. 2, pp. 263-278, 2006.

[53] S. Ozkan and B. Karabacak, "Collaborative risk method for information security management practices: A case context within Turkey", International Journal of Information Management, vol. 30, no. 6, pp. 567-572, 2010.